UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/713,180	11/13/2003	Hidetada Nago	1232-5208	9816

27123 7590 10/09/2007
MORGAN & FINNEGAN, L.L.P.
3 WORLD FINANCIAL CENTER
NEW YORK, NY 10281-2101

EXAMINER	
HOLLIDAY, JAIME MICHELE	
ART UNIT	**PAPER NUMBER**
2617	

NOTIFICATION DATE	DELIVERY MODE
10/09/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTOPatentCommunications@Morganfinnegan.com
Shopkins@Morganfinnegan.com
jmedina@Morganfinnegan.com

Office Action Summary	Application No.	Applicant(s)	
	10/713,180	NAGO, HIDETADA	
	Examiner	Art Unit	
	Jaime M. Holliday	2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 September 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) *2,3,6-12,15 and 16* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 4, 5, 13, 14 and 17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on September 20, 2007 has been entered.

Response to Amendment

Response to Arguments

2. Applicant's arguments filed September 20, 2007 have been fully considered but they are not persuasive.

Applicant basically argues that the cited prior art fail to disclose or suggest a "scheme for limiting printers that can read Service Set ID from the wireless LAN adapter to use the wireless LAN adapter." In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., limiting printers that can read Service Set ID) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Further, Applicant also argues that the cited prior art fail to disclose a "comparison step," "notification step," and/or a "second reading step." Examiner respectfully disagrees in view of the Sato reference. Sato discloses that the controller determines whether an address of the management device is included in the IC card, and if included, calls that address via the communication port, and performs a communications test. If the controller can communicate with the management device, the controller determines that the set communication parameters are valid, and completes the communications test. In this case, the management device transmits to the network apparatuses notification (response confirming completion) that test communications from the controller have been responded to. On the other hand, if the controller cannot communicate with the management device, the controller determines that the set communication parameters are invalid, and completes the communications test. The controller, if required, may transmit the device information and/or the security information (i.e., user ID and password pairs) upon communications test, reading on the "comparison, notification and second reading" steps.

Therefore, in view of the preceding arguments, Examiner maintains rejection.

Claim Rejections - 35 USC § 103

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. **Claims 1, 4, 5, 13, 14 and 17** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Noda (U.S. 2005/0015467 A1)** in view of **Sato (U.S. 2003/0009541 A1)** in view **Bartolome et al. (U.S. 7,149,805 B2)**.

Consider **claims 1 and 7**, Noda clearly shows and discloses communication apparatus and method that allow setting for forming a wireless link. A personal computer **1**, reading on the claimed "external computer," includes a CPU (central processing unit) **11**, which is connected to an input/output interface **15** via a bus **14**, and furthermore, a ROM (read only memory) **12** and a RAM (random access memory) **13** are connected to the bus. An IC-card contactless communication unit **19** for detecting an IC card **2**, reading on the claimed "wireless LAN adapter having a wireless communication unit and a memory," when it is placed in close proximity thereto and reading data from and writing data to the IC card, a wireless communication unit **20** for forming a wireless link and exchanging data with, for example, the access-point device **3**, by a wireless communication function conforming to IEEE 802.11b, according to access-point information, local-network information, or the like that is set by the CPU, (abstract, paragraphs 52-53). The personal computer **1-1**, reading on the claimed "external computer," starts processing when a user performs an operation for requesting that local-network information required for the personal computer **1-2**, reading on the claimed "first apparatus," to form a wireless link with the personal computer be recorded in the IC card. When the user places the IC card in proximity to the IC-card contactless communication unit **19-1** of the

personal computer, the IC-card contactless communication unit detects the IC card, and the IC-card contactless communication unit records the local-network information required for the personal computer **1-2** to form a wireless link with the personal computer **1-1** in the IC card, reading on the claimed "registration step," (paragraphs 78 and 80). The personal computer requires an SSID and a WEP KEY defined in IEEE 802.11b to be set before forming a wireless link with the access-point device, reading on the claimed "causing an external computer apparatus to register Service Set ID of a target printer to use the wireless LAN adapter into the memory, in a case that the external computer apparatus is connected to the wireless LAN adapter, wherein the Service Set ID defines wireless LAN communication of the target printer," (abstract, paragraph 50). When the user places the IC card in proximity to the IC-card contactless communication unit **19-2** of the personal computer **1-2**, the IC-card contactless communication unit detects the IC card, and determines whether local-network information is recorded in the IC card. If it is determined that local-network information is recorded in the IC card, the IC-card contactless communication unit reads the local-network information recorded in the IC card, reading on the claimed "a second reading step of causing the printing apparatus to read the Service Set ID from the memory of the wireless LAN adapter." The CPU **11-2** sets network configuration of the wireless communication unit **20-2** according to the local-network information read by the IC-card contactless communication unit, reading on the claimed "setting step causing the [printing] apparatus to set

the Service Set ID read in said second reading step in the wireless LAN communication unit of the wireless LAN adapter connected to the [printing] apparatus." Thus, a wireless LAN is formed between the personal computer **1-1** and the personal computer **1-2** in ad-hoc mode, reading on the claimed "communication method for allowing a [printing] apparatus connected to a wireless LAN adapter having a wireless communication unit and a memory, to perform wireless LAN communication, said communication method comprising a communication step of performing wireless LAN communication using the Service Set ID set," (paragraphs 84 and 85).

However, Noda fails to disclose comparing information with identification already stored on the printer.

In the same field of endeavor, Sato clearly shows and discloses a network system that comprises a target device to be managed that is connected to a network, and a management device that manages the target device, wherein the management device enables the target device to establish communications over the network and includes a first integrated circuit (IC) card drive in which an IC card stores communication parameters for enabling the management device to manage the target device, and wherein the target device includes a second IC card drive for reading the communication parameters stored in the IC card to set the communication parameters that have been read. The network system uses the IC card as a relay to perform an initial setting of the communication parameters on the target device. This enables the communication parameters to

be set only by insertion of the IC card into the target device, achieving a relatively easy setting operation, (paragraph 10). When a user of the management device **10** withdraws an IC card **50** from the IC card driver **20** of the management device, and carries and inserts the IC card into the IC card driver **70** of the network apparatus **60**, the controller **61** reads and sets some of the communication parameters stored in the IC card corresponding to the pertinent network apparatus. More specifically, the controller sets the communication parameters obtained through the IC card drive and the interface **66** on the storage part **65** (paragraphs 71-75). The management device may further store an address of the management device in the IC card, and the above target device may call the address to communicate with the management device after setting the communication parameters. This allows the target device to communicate with the management device to confirm the setting of the communication parameters. Moreover, the target device, when communicating with the management device, may transmit the device information unique to the target device to the management device, and the management device may store the device information unique to the target device. This allows the management device to manage the communication parameters and device information of the target device, reading on the claimed "causing an external computer to register printer ID of a target printer to use the wireless LAN adapter; a first reading step of causing the printing apparatus to read printer ID from the memory, in a case that the wireless LAN adapter in which the printer ID has been registered in said

registration step is connected to the printing apparatus," (paragraph 12). The controller **61** determines whether an address of the management device **10** is included in the IC card **50**, and if included, calls that address via the communication port **62**, and performs a communications test. If the controller can communicate with the management device, the controller determines that the set communication parameters are valid, and completes the communications test. In this case, the management device transmits to the network apparatuses notification (response confirming completion) that test communications from the controller have been responded to. On the other hand, if the controller cannot communicate with the management device, the controller determines that the set communication parameters are invalid, and completes the communications test. The controller, if required, may transmit the device information and/or the security information (i.e., user ID and password pairs) upon communications test, reading on the claimed "a comparison step of comparing the printer ID read in said first reading step with printer ID of the printing apparatus preset in the printing apparatus; a notification step of notifying a user of an error, in a case that the printer ID of the printing apparatus does not match with printer ID read in said first reading step," (paragraph 85).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate a step of verifying user ID and password, along with device information and communication parameters, as

taught by Sato, in the system of Noda, in order to form a wireless link between two apparatuses in a wireless system.

However, Noda, as modified by Sato, fails to specifically disclose the PC's communicating via the IC-card contactless communication unit.

In the same field of endeavor, Bartolome et al. clearly show and disclose a communication system that may include one or more wireless devices **304**, a network member fixed computer device **311**, and a computer network **318**. The wireless device may be any type of mobile wireless device capable of communicating in a wireless manner with other wireless devices. This may include radio frequency communication and may additionally include infrared communication. The wireless device may be, for example, a cellular telephone, a pager, a laptop or notebook computer, a pager, a personal digital assistant (PDA), etc. The network member device is not itself a wireless infrastructure device. For example, the network member device 311 may be a personal computer, a network workstation, a dumb terminal, a printer, a copier, a scanner, a facsimile, a disk or tape drive, a disk drive server, etc., reading on the claimed "printing apparatus." The computer network may be a local area network (LAN), a wide area network (WAN), a virtual private network (VPN), etc., reading on the claimed wireless LAN communication," (col. 3 lines 10-50). The network member device may include a wireless communication card **417** that further includes a modem card **424** and an associated antenna **403** and a bridge **429**. The modem card may be any type of standard modem card capable of

communicating with a wireless device. The modem card performs data conversion and performs wireless transmission and reception of data, such as through radio frequency (RF) communications. The modem card may operate according to any known wireless protocol, such as cellular formats, BLUETOOTH, etc., reading on the claimed "wireless LAN adapter." In operation, the modem card conducts wireless communications with one or more wireless devices, reading on the claimed "communication step of causing the wireless communication unit of the wireless LAN adapter connected to the printing apparatus to perform the wireless LAN communication," (col. 5 lines 25-55, col. 6 lines 21-23).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate a modem card in a fixed apparatus that can communicate wirelessly with a mobile device as taught by Bartolome et al., in the system of Noda, as modified by Sato, in order to form a wireless link between two apparatuses in a wireless system.

Consider **claim 4**, the combination of Noda and Sato, as modified by Bartolome et al., clearly shows and discloses the claimed invention **as applied to claim 1 above**, and in addition, Sato further disclose that the communication parameters may include cryptographic information (e.g., key information and encryption scheme), reading on the claimed "external computer apparatus further registers an encryption key for encryption communication by the printing apparatus in the memory of the wireless LAN adapter," (paragraph 44).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include encryption information within the communication parameters which are set, as taught by Sato, in the system of Noda, in order to form a secure wireless link between two apparatuses in a wireless system.

Consider **claim 5**, the combination of Noda and Sato, as modified by Bartolome et al., clearly shows and discloses the claimed invention **as applied to claim 4 above**, and in addition, Sato further disclose that if the controller can communicate with the management device, the controller determines that the set communication parameters are valid, and completes the communications test, reading on the claimed "wherein said second reading step causes the printing apparatus to read the Service Set ID associated with the printer ID of printing apparatus from the memory," (paragraph 44). In order to test if the information is valid, the stored information is "read" and "compared" to retrieved information.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate a step of verifying user ID and password, along with device information and communication parameters, as taught by Sato, in the system of Noda, in order to form a wireless link between two apparatuses in a wireless system.

Consider **claims 13 and 17**, Noda clearly shows and discloses communication apparatus and method that allow setting for forming a wireless link. A personal computer, reading on the claimed "external computer

apparatus," includes a CPU (central processing unit), which is connected to an input/output interface via a bus, and furthermore, a ROM (read only memory) and a RAM (random access memory) are connected to the bus. An IC-card contactless communication unit for detecting an IC card, reading on the claimed "wireless LAN adapter," when it is placed in close proximity thereto and reading data from and writing data to the IC card, a wireless communication unit for forming a wireless link and exchanging data with, for example, the access-point device, by a wireless communication function conforming to IEEE 802.11b, according to access-point information, local-network information, or the like that is set by the CPU, (abstract, paragraphs 52-53). A first communication apparatus that includes wireless communication means for carrying out wireless communication with another electronic apparatus based on a predetermined wireless communication standard and reading means for reading the setting information, by contactless communication, from an information recording medium detected by a detection means. Since the access-point device is capable of writing data to the IC card, it is possible to additionally record user information for forming a link with a wireless LAN that is formed via the access-point device, (fig. 1, paragraphs 10 and 69). When the user places the IC card in proximity to the IC-card contactless communication unit **19-2** of the personal computer **1-2**, the IC-card contactless communication unit detects the IC card, and determines whether local-network information is recorded in the IC card. The personal computer requires an SSID and a WEP KEY defined in IEEE 802.11b to

be set before forming a wireless link with the access-point device, reading on the claimed "register Service Set ID," (abstract, paragraph 50). If it is determined that local-network information is recorded in the IC card, the IC-card contactless communication unit reads the local-network information recorded in the IC card. The CPU **11-2** sets network configuration of the wireless communication unit **20-2** according to the local-network information read by the IC-card contactless communication unit. Thus, a wireless LAN is formed between the personal computer **1-1** and the personal computer **1-2** in ad-hoc mode, reading on the claimed "[printing] apparatus which is capable of performing wireless LAN communication by being connected with a wireless LAN adapter having a wireless LAN communication unit and a memory, comprising a detection unit configured to detect a connection with the wireless LAN adapter; a second reading unit configured to read Service Set ID from the memory, in a case that the printer ID of the printing apparatus matches with the printer ID read by said first reading unit, wherein the Service Set ID is registered in the memory by the external computer apparatus; a setting unit configured to set the Service Set ID read by said second reading unit in the wireless LAN communication unit of the wireless LAN adapter connected to the [printing] apparatus as wireless communication parameters for which the wireless LAN communication unit performs the wireless LAN communication, and wireless communication means for performing the wireless LAN communication using LAN the Service Set ID set in the wireless communication unit," (paragraphs 84 and 85).

However, Noda fails to disclose comparing information with identification already stored on the printer.

In the same field of endeavor, Sato clearly shows and discloses a network system that comprises a target device to be managed that is connected to a network, and a management device that manages the target device, wherein the management device enables the target device to establish communications over the network and includes a first integrated circuit (IC) card drive in which an IC card stores communication parameters for enabling the management device to manage the target device, and wherein the target device includes a second IC card drive for reading the communication parameters stored in the IC card to set the communication parameters that have been read. The network system uses the IC card as a relay to perform an initial setting of the communication parameters on the target device. This enables the communication parameters to be set only by insertion of the IC card into the target device, achieving a relatively easy setting operation, (paragraph 10). When a user of the management device **10** withdraws an IC card **50** from the IC card driver **20** of the management device, and carries and inserts the IC card into the IC card driver **70** of the network apparatus **60**, the controller **61** reads and sets some of the communication parameters stored in the IC card corresponding to the pertinent network apparatus. More specifically, the controller sets the communication parameters obtained through the IC card drive and the interface **66** on the storage part **65** (paragraphs 71-75). The management device may further store

an address of the management device in the IC card, and the above target device may call the address to communicate with the management device after setting the communication parameters. This allows the target device to communicate with the management device to confirm the setting of the communication parameters. Moreover, the target device, when communicating with the management device, may transmit the device information unique to the target device to the management device, and the management device may store the device information unique to the target device. This allows the management device to manage the communication parameters and device information of the target device, reading on the claimed "a first reading unit configured to read printer ID from the memory of the wireless LAN adapter, wherein the printer ID is registered as a printer identifier of a target printer to use the wireless LAN adapter in the memory by an external computer apparatus, in a case that said detection unit detects that the wireless LAN adapter is connected to the printing apparatus," (paragraph 12). The controller **61** determines whether an address of the management device **10** is included in the IC card **50**, and if included, calls that address via the communication port **62**, and performs a communications test. If the controller can communicate with the management device, the controller determines that the set communication parameters are valid, and completes the communications test. In this case, the management device transmits to the network apparatuses notification (response confirming completion) that test communications from the controller have been responded

to. On the other hand, if the controller cannot communicate with the management device, the controller determines that the set communication parameters are invalid, and completes the communications test. The controller, if required, may transmit the device information and/or the security information (i.e., user ID and password pairs) upon communications test, reading on the claimed "a comparison unit configured to compare the printer ID read by said first reading unit with printer ID of the printing apparatus preset in the printing apparatus; a notification unit configured to notify a user of an error, in a case that the printer ID of the printing apparatus does not match with printer ID read by said first reading unit," (paragraph 85).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate a step of verifying user ID and password, along with device information and communication parameters, as taught by Sato, in the system of Noda, in order to form a wireless link between two apparatuses in a wireless system.

However, Noda, as modified by Sato, fails to specifically disclose the PC's communicating via the IC-card contactless communication unit.

In the same field of endeavor, Bartolome et al. clearly show and disclose a communication system that may include one or more wireless devices **304**, a network member fixed computer device **311**, and a computer network **318**. The wireless device may be any type of mobile wireless device capable of communicating in a wireless manner with other wireless devices. This may

include radio frequency communication and may additionally include infrared communication. The wireless device may be, for example, a cellular telephone, a pager, a laptop or notebook computer, a pager, a personal digital assistant (PDA), etc. The network member device is not itself a wireless infrastructure device. For example, the network member device 311 may be a personal computer, a network workstation, a dumb terminal, a printer, a copier, a scanner, a facsimile, a disk or tape drive, a disk drive server, etc., reading on the claimed "printing apparatus." The computer network may be a local area network (LAN), a wide area network (WAN), a virtual private network (VPN), etc., reading on the claimed wireless LAN communication," (col. 3 lines 10-50). The network member device may include a wireless communication card **417** that further includes a modem card **424** and an associated antenna **403** and a bridge **429**. The modem card may be any type of standard modem card capable of communicating with a wireless device. The modem card performs data conversion and performs wireless transmission and reception of data, such as through radio frequency (RF) communications. The modem card may operate according to any known wireless protocol, such as cellular formats, BLUETOOTH, etc., reading on the claimed "wireless LAN adapter." In operation, the modem card conducts wireless communications with one or more wireless devices, reading on the claimed "printing apparatus connected to the wireless LAN adapter performs wireless LAN communication via a wireless

communication unit of the wireless LAN adapter," (col. 5 lines 25-55, col. 6 lines 21-23).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate a modem card in a fixed apparatus that can communicate wirelessly with a mobile device as taught by Beach, in the system of Noda, in order to form a wireless link between two apparatuses in a wireless system.

Consider **claim 14**, the combination of Noda and Sato, as modified by Bartolome et al., clearly show and disclose the claimed invention **as applied to claim 13 above**, and in addition, Noda further discloses a first communication apparatus that includes wireless communication means for carrying out wireless communication with another electronic apparatus based on a predetermined wireless communication standard, reading means for reading the setting information, by contactless communication, from an information recording medium detected by a detection means, and setting means for adjusting setting of the wireless communication means according to the setting information read by the reading means, (fig. 1, paragraphs 10 and 69). The setting information may include at least one of ID information, a password associated with the ID information, a user name, and a password associated with the user name and ID information SSID, reading on the claimed "wherein said second reading unit reads the Service Set ID from the memory, and wherein said setting unit sets the

Service Set ID read by the second reading unit in the wireless LAN communication unit of the wireless LAN adapter," (paragraphs 15, 81).

However, Noda fails to disclose that the setting encryption information.

In the same field of endeavor, Sato further disclose that the communication parameters may include cryptographic information (e.g., key information and encryption scheme), reading on the claimed "wherein said second reading unit reads an encryption key fro encryption communication from the memory, wherein the encryption key is registered in the memory by the external computer apparatus, and wherein said setting unit sets the encryption key read by the second reading unit in the wireless LAN communication unit of the wireless LAN adapter," (paragraph 44).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include encryption information within the communication parameters which are set, as taught by Sato, in the system of Noda, in order to form a secure wireless link between two apparatuses in a wireless system.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jaime M. Holliday whose telephone number is (571)

272-8618. The examiner can normally be reached on Monday through Friday 7:30am to 4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Feild can be reached on (571) 272-4090. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jaime Holliday
Patent Examiner

JEAN GELIN
PRIMARY EXAMINER